IN THE UNITED STATED DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

M.C., individually and on behalf of all similarly situated persons,

Plaintiff,

v.

EAST SIDE HEALTH DISTRICT

Defendant.

Civil Action No. 3:24-CV-01336-NJR

FIRST AMENDED CLASS ACTION COMPLAINT

COMES NOW Plaintiff M.C. ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant East Side Health District ("ESHD"), an Illinois corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action brought by Plaintiff and the Class, individually and on behalf of all those similarly situated (*i.e.*, the Class Members), seeking to redress Defendant's willful and reckless violations of their privacy rights. Plaintiff was a patient of ESHD who entrusted her Protected Health Information ("PHI") and Personally Identifiable Information ("PII") to Defendant. Defendant betrayed Plaintiff's and the Class Members' trust by failing to properly safeguard and protect their PHI and PII and publicly disclosing their PHI and PII without

authorization in violation of Illinois common law.

2. This class action is in regard to recent targeted cyberattack and data breach ("Data Breach") at ESHD, an Illinois health-care network that offers clinical care services. As a result of the Data Breach, Plaintiff and tens of thousands of Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

3. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant for safe keeping —was compromised and unlawfully accessed due to the Data Breach.

4. Information compromised in the Data Breach includes names, contact information, dates of birth, treatment and diagnosis information test result(s), prescription information, date(s) of service, provider name(s), health insurance information, and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively the "Private Information").

5. Defendant disclosed Plaintiff's and Class Members' PHI and PII to unauthorized persons as a direct and/or proximate result of Defendant's failure to safeguard and protect their PHI and PII.

6. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiff's and Class Members' names, contact information, dates of birth, treatment and diagnosis information, test result(s), prescription information, date(s) of service, provider name(s) and/or health insurance information.

7. Defendant flagrantly disregarded Plaintiff's and Class Members' privacy and

property rights by intentionally, willfully and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiff's and the Class Members' PHI and PII from unauthorized disclosure. Plaintiff's and Class Members' PHI and PII was improperly handled, inadequately protected, and not kept in accordance with basic security protocols. Defendant's obtaining of the information and sharing of same also represent a flagrant disregard of Plaintiff's and Class Members' rights, both as to privacy and property.

8. Plaintiff and the Class would not have provided their PHI and PII to Defendant if they had known Defendant would not protect the information as it promised to do.

9. Plaintiff has standing to bring this action because as a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, Plaintiff and the Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy and/or (ii) the additional damages set forth in detail below, which are incorporated herein by reference.

10. Defendant's wrongful actions and/or inaction and the resulting Breach have also placed Plaintiff and the Class at an imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud. Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released its 2012 Identity Fraud Report ("the Javelin Report"), quantifying the impact of breaches. According to the Javelin Report, individuals whose PHI and PII are subject to a reported breach—such as the Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiff's and the Class Members' PII and not yet used the information will do so at a later date

or re-sell it.

11. Plaintiff and the Class have also suffered and are entitled to damages for the lost benefit of their bargains with Defendant. Plaintiff and the Class Members paid Defendant for their services including it protecting their PHI and PII. The lost benefit of the bargain is measured by the difference between the value of what Plaintiff and the Class should have received when they paid for Defendant's services, and the value of what they actually did receive: services without adequate privacy safeguards. Plaintiff and the Class have been harmed in that they (1) paid more for privacy and confidentiality than they otherwise would have, and (2) paid for privacy protections they did not receive. In that respect, Plaintiff and the Class have not received the benefit of their bargains and have suffered an ascertainable loss.

12. Additionally, because of Defendant's conduct, Plaintiff and the Class have been harmed in that Defendant has breached its common law fiduciary duty of confidentiality owed to Plaintiff and the Class.

13. Accordingly, Plaintiff and the Class seek redress against Defendant for breach of implied contract, breach of contract, common law negligence.

14. Plaintiff and the Class seek all (i) actual damages, economic damages, (ii) injunctive relief, and (iii) attorneys' fees, litigation expenses, and costs.

PARTIES

15. Plaintiff M.C. is an adult individual residing in Swansea, St. Clair County, Illinois.

16. At all relevant times, Defendant ESHD has been a corporation which provides health services to East St. Louis, Illinois residents. Defendant's headquarters is located at 639 N 20th St., East St. Louis, Illinois 62205.

JURISDICTION AND VENUE

1. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

2. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant conducts much of their business in this District and Defendant has caused harm to Class Members residing in this District.

BACKGROUND FACTS

17. Certain allegations are made upon information and belief.

18. Defendant ESHD is a health care provider pursuant to state and federal law, providing health care and medical services to the general public, including Plaintiff.

19. As a part of their business operations, Defendant collect and maintain PHI and PII of their patients.

20. Plaintiff and the Class are and/or were patients of Defendant ESHD and, as a result, provided their PHI and PII to Defendant.

21. Plaintiff and the Class entered into an implied contract with Defendant for the adequate protection of their PHI and PII.

22. Defendant is required to maintain the strictest privacy and confidentiality of Plaintiff's and the Class Members' medical records and other PHI and PII.

23. Defendant is required to post its privacy practices online. However, they currently have no such privacy practices posted.

24. Between December 1, 2023, and December 8, 2023, Defendant, "…learned of an incident that disrupted the operations of some of our IT systems."

25. Defendant subsequently sent a letter, on or around February 2, 2024, to Plaintiff and the Class notifying them of the Breach.

26. The Breach letter notified patients that, "[o]ur investigation determined that an unauthorized party accessed some of our systems between December 1, 2023, and December 8, 2023, and accessed or removed certain files."

27. ESHD issued a "Notice of Data Privacy Incident" on their website which can be found here: https://eastsidehealthdistrict.org/notice-of-data-privacy-incident/

28. The disclosure of the PHI and PII at issue was a result of the Defendant's inadequate safety and security protocols governing PHI and PII.

29. Defendant's lack of investigation regarding the egregious disclosure of Plaintiff's and the Class's highly sensitive medical information is a gross disregard to the Plaintiff's and the Class's concerns of their privacy.

30. The disclosure of the PHI and PII at issue was a result of the Defendant's inadequate safety and security protocols governing PHI and PII.

31. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiff's and the Class Members' names, contact information, dates of birth, treatment and diagnosis information, test result(s), prescription information, date(s) of services, provider name(s) and/or health insurance information.

32. As a direct and/or proximate result of Defendant's failure to properly safeguard and protect the PHI and PII of their patients and their parents/guardians, Plaintiff's and the Class Members' PHI and PII was stolen, compromised, and wrongfully disseminated without authorization.

33. Defendant has a duty to its patients to protect them from wrongful disclosures.

34. As a health care provider, Defendant is required to train and supervise their employees regarding the policies and procedures as well as the State and Federal laws for safeguarding patient information.

35. Defendant is a covered entity pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

36. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH")[1]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

37. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy Illinois. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

38. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

39. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. *See* 42 C.F.R. §§ 164.302-164.318.

40. HIPAA limits the permissible uses of "protected health information" and prohibits

[1] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

41. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

42. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

43. Under HIPAA:

> Protected health information means individually identifiable health information:
>
> (1) Except as provided in paragraph (2) of this definition, that is:
>
> (i) Transmitted by electronic media;
>
> (ii) Maintained in electronic media; or
>
> (iii) Transmitted or maintained in any other form or medium.[2]

[2] 45 C.F.R. § 160.103

44. HIPAA and HITECH obligated Defendant to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

45. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

46. HIPAA further obligated Defendant to ensure that its workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train their workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

47. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance

Material.[3] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[4]

48. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);
>
> (2) the recipient of the PHI;
>
> (3) whether the PHI was actually acquired or viewed; and
>
> (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[5]

49. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

[3] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
[4] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
[5] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

50. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train their employees and staff so that all their staff and employees know their roles in facility security.

51. Defendant failed to provide timely and proper notice to Plaintiff and the Class of the disclosure.

52. Defendant failed to conduct or improperly conducted the four-factor risk assessment following the unauthorized disclosure.

53. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, unauthorized individuals now have Plaintiff's and the Class Members' compromised PHI and PII.

54. There is a robust international market for the purloined PHI and PII, specifically medical information. Defendant's wrongful actions and/or inaction and the resulting Breach have also placed Plaintiff and the Class Members at an imminent, immediate, and continuing increased risk of identity theft, identity fraud[6] and medical fraud.

55. Identity theft occurs when someone uses an individual's PHI and PII, such as the person's name, Social Security number, or credit card number, without the individual's permission, to commit fraud or other crimes. *See* Federal Trade Commission, Fighting Back against Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/ about-identity-theft.html (last visited Jan. 18, 2013). The Federal Trade Commission estimates that the identities of as many as nine million Americans are stolen each year. *Id.*

[6] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia,* credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

56. The Federal Trade Commission correctly sets forth that "Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit." *Id.*

57. Identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (such as obtaining a driver's license or official identification card in the victim's name but with their picture), using a victim's name and Social Security number to obtain government benefits and/or filing a fraudulent tax return using a victim's information. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments and/or obtain medical services in a victim's name. Identity thieves also have been known to give a victim's PHI and PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

58. According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[7] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[8]

[7] *Protecting Consumer Privacy in an Era of Rapid Change* FTC, Report March 2012 (http://www.ftc.gov/os/2012/03/120326privacyreport.pdf).

[8] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report*, 35-38 (Dec. 2010), *available at*

59. According to the Javelin Report, in 2011, the mean consumer cost of rectifying identity fraud was $354 while the mean resolution time of identity fraud was 12 hours. *Id.* at 6. In 2011, the consumer cost for new account fraud and existing non-card fraud increased 33% and 50% respectively. *Id.* at 9. Consumers who received a breach notification had a fraud incidence rate of 19% in 2011 and, of those experiencing fraud, 43% reported their credit card numbers were stolen and 22% of the victims reported their debit card numbers were stolen. *Id.* at 10. More important, consumers who were notified that their PHI and PII had been breached were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification. *Id.* at 39.

60. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse. *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327 (http://www.ssa.gov/pubs/10064.html). Thus, a person whose PII has been stolen cannot obtain a new Social Security number until the damage has already been done.

61. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems; because

---

http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12.

prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

62. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods. *See* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html. For example, as of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn, has led to a surge in medical identity theft as a means of fraudulently obtaining medical care. "Victims of medical identity theft [also] may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits." *Id.*

63. Defendant flagrantly disregarded and/or violated Plaintiff's and the Class's privacy and property rights, and harmed them in the process, by not obtaining Plaintiff's and the Class Members' prior written consent to disclose their PHI and PII to any other person—as required by laws, regulations, industry standards and/or internal department standards.

64. Defendant flagrantly disregarded and/or violated Plaintiff's and the Class's privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiff's and the Class Members' PHI and PII to unauthorized persons.

65. Upon information and belief, Defendant flagrantly disregarded and/or violated Plaintiff's and the Class Members' privacy and property rights, and harmed them in the process, by failing to keep or maintain an accurate accounting of the PHI and PII wrongfully disclosed in the Breach.

66. Defendant flagrantly disregarded and/or violated Plaintiff's and the Class

Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and the Class's PHI and PII to protect against anticipated threats to the security or integrity of such information. Defendant's unwillingness or inability to establish and maintain the proper information security procedures and controls is an abuse of discretion and confirms their intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

67. As a result of the Data Breach, Plaintiff has experienced fraudulent charges on her financial accounts which she has had to dispute. Plaintiff also has been inundated with phishing emails and spam emails and texts.

68. Plaintiff has received no other notices of Data Breach other than the one at issue in this case.

69. The actual harm and adverse effects to Plaintiff and the Class, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's above wrongful actions and/or inaction and the resulting Breach requires Plaintiff and the Class to take affirmative acts to recover their peace of mind, and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts—for which there is a financial and temporal cost. Plaintiff and the Class have suffered, and will continue to suffer, such damages for the foreseeable future.

70. Victims and potential victims of identity theft, identity fraud and/or medical

fraud—such as Plaintiff and the Class—typically spend hundreds of hours in personal time and hundreds of dollars in personal funds to resolve credit and other financial issues resulting from breaches. *See Defend: Recover from Identity Theft*, http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/defend.html; *Fight Identity Theft*, www.fightidentitytheft.com. According to the Javelin Report, not only is there a substantially increased risk of identity theft and identity fraud for breach victims, those who are further victimized by identity theft or identity fraud will incur an average fraud-related economic loss of $1,513 and incur an average of $354 of out-of-pocket expenses attempting to rectify the situation. *Id*. at 6.

71. Other statistical analyses are in accord. The GAO found that identity thieves use PHI and PII to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PHI and PII, Social Security numbers are incredibly difficult to change, and their misuse can continue for years into the future. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

72. Defendant's wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, Plaintiff and the Class have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) the imminent, immediate and continuing increased risk of identity theft, identity fraud and/or medical

fraud, (iii) out-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance and/or other Breach risk mitigation products, (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach, including the costs of placing a credit freeze and subsequently removing a credit freeze, (v) the value of their time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach and (vi) the lost benefit of their bargains when they paid for their privacy to be protected and it was not.

CLASS ACTION ALLEGATIONS

73. Pursuant to 735 ILCS 5/2-801 Plaintiff brings this class action as a class action on behalf of themself and the following class:

> **National Class:** All persons residing in the United States who were patients of Defendant ESHD whose PHI and/or PII was disclosed by Defendant to unauthorized third-parties between December 1, 2023 and December 8, 2023.
>
> **Illinois Class:** All persons residing in the United States who were residents of Illinois who were patients of Defendant ESHD whose PHI and/or PII was disclosed by Defendant to unauthorized third-parties between December 1, 2023 and December 8, 2023.

74. Excluded from the Class are the following individuals and/or entities:

> Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

75. Numerosity: On information and belief, the putative Class are comprised of tens of thousands of individuals making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

76. Commonality and Predominance: The rights of Plaintiff and each other Class Members were violated in a virtually identical manner as a direct and/or proximate result of Defendant's 'willful, reckless and/or negligent actions and/or inaction and the resulting Breach. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a. Whether Defendant willfully, recklessly and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff and the other Class Members' PHI and/or PII;

b. Whether Defendant was negligent in failing to properly safeguard and protect Plaintiff's and the other Class Members' PHI and/or PII;

c. Whether Defendant owed a duty to Plaintiff and the other Class Members to exercise reasonable care in safeguarding and protecting their PHI and/or PII;

d. Whether Defendant breached its duty to exercise reasonable care in failing to safeguard and protect Plaintiff's and the other Class Members' PHI and/or PII;

e. Whether Defendant was negligent in failing to safeguard and protect Plaintiff's and the other Class Members' PHI and/or PII;

f. Whether, by publicly disclosing Plaintiff's and the other Class Members' PHI and/or PII without authorization, Defendant invaded their privacy; and

g. Whether Plaintiff and the other Class Members sustained damages as a result of Defendant's failure to safeguard and protect their PHI and/or PII.

77. Adequacy: Plaintiff and their counsel will fairly and adequately represent the interests of the other Class Members. Plaintiff has no interests antagonistic to, or in conflict with,

the other Class Members' interests. Plaintiff's lawyers are highly experienced in the prosecution of consumer class action and data breach cases.

78. Typicality: Plaintiff's claims are typical of the other Class Members' claims in that Plaintiff's claims and the other Class Members' claims all arise from Defendant's failure to properly safeguard and protect their PHI and PII.

79. Superiority and Manageability: A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff's and the other Class Members' claims. Plaintiff and the other Class Members have been harmed as a result of Defendant's wrongful actions and/or inaction and the resulting Breach. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct.

80. Class certification, therefore, is appropriate pursuant to 735 ILCS 5/2-801 as the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

81. Policies Generally Applicable to the Case: Class certification also is appropriate pursuant to 735 ILCS 5/2-801 because Defendant have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

82. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights. Absent a class action, Defendant will retain the benefits of their wrongdoing despite their serious violations of the law.

83. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

84. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

85. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

COUNT I
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class and the Illinois Class)

86. The preceding factual statements and allegations are incorporated herein by reference.

87. Plaintiff and the other Class Members, as part of their agreement with Defendant provided Defendant their PHI and PII.

88. In providing such PHI and PII, Plaintiff and the other Class Members entered into an implied contract with Defendant, whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class members' PHI and PII.

89. Under the implied contract, Defendant were obligated to not only safeguard the PHI and PII, but also to provide Plaintiff and Class Members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

90. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their PHI and PII.

91. As a direct result of Defendant's breach of their duty of confidentiality and privacy and the disclosure of Plaintiff's and the other Class Members' confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of time, suffered fraud and misuse of their information, suffered identity theft, exposure to heightened future risk of identity theft, loss of privacy and confidentiality.

92. Plaintiff and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; and, (vi) the increased risk of identity theft. At the very least, Plaintiff and Class Members are entitled to nominal damages.

COUNT II
NEGLIGENCE
(On behalf of Plaintiff and the Class and the Illinois Class)

93. The preceding factual statements and allegations are incorporated herein by reference.

94. Plaintiff brings this Count on their own behalf and on behalf of the Class (the "Class" for the purposes of this Count).

95. Defendant owed, and continue to owe, a duty to Plaintiff and the Class to safeguard and protect their PHI and PII.

96. Defendant breached its duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiff's and the other Class Members' PHI and PII.

97. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PHI and PII would result in an unauthorized third-party gaining access to such information for no lawful purpose.

98. Plaintiff and the Class entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third-parties.

99. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Class could and would suffer if the PII and PHI were wrongfully disclosed.

100. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third-party.

101. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

102. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients', employees', and physicians' PII and PHI that Defendant were no longer required to retain pursuant to regulations.

103. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and the Class.

104. Defendant's duty to use reasonable security measures arose as a result of the contractual relationship that existed between Defendant and Plaintiff and the Class.

105. Defendant was also subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

106. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

107. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting or redacting PII and PHI stored on Defendant's systems.

108. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class.

109. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions to not comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

110. Plaintiff and the Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

111. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Disclosure/Data Breach. Defendant had and continues to have a duty to

adequately disclose that the PII and PHI of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third-parties.

112. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Class.

113. Defendant have admitted that the PII and PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third-persons as a result of the Disclosure/Data Breach.

114. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry standard protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Class during the time the PII and PHI was within Defendant's possession or control.

115. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Disclosure/Data Breach.

116. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and the Class in the face of increased risk of theft.

117. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of their current and former patients', employees', and physicians' PII and PHI.

118. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Disclosure/Data Breach.

119. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the members of the Class confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

120. Plaintiff and the other Class suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

121. Defendant's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) negligence at common law. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard. Defendant violated Section 5

of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

122. Defendant's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

123. Defendant's violation of Section 5 of the FTC Act and Title II of HIPAA, including HIPAA regulations HHS has implemented pursuant to Title II, as well as the standards of conduct established by these statutes and regulations, constitutes negligence per se.

124. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

125. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

126. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. fraud and misuse of their information;

c. the loss of the opportunity of how their PII and PHI is used;

d. the compromise, publication, and/or theft of their PII and PHI;

e. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI;

f. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

g. costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Class; and

h. costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

127. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

128. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII and PHI,

which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in their continued possession.

129. Plaintiff and the Class are therefore entitled to damages, including actual and compensatory damages, restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff and the Class respectfully request that the Court enter judgment in their favor and against each Defendant, as follows:

A. Declaring that Defendant breached their implied contract with Plaintiff and the Class;

B. Declaring that Defendant negligently disclosed Plaintiff's and the Class Members' PHI and PII;

C. Ordering Defendant to pay actual damages to Plaintiff and the Class;

D. Ordering Defendant to disseminate individualized notice of the Breach to Plaintiff and the Class;

E. For an Order enjoining Defendant from continuing to engage in the unlawful business practices alleged herein;

F. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiff and the Class;

G. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

H. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiff and the Class respectfully demand a trial by jury on all of their claims and causes of action so triable.

Respectfully submitted,

Maureen M. Brady MO#57800
Lucy McShane MO#57957
MCSHANE & BRADY, LLC
4006 Central Street
Kansas City, MO 64111
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com
ATTORNEYS FOR PLAINTIFF AND THE PROPOSED CLASS